

The Emma Red Company

Data Protection Policy

The Emma Red Company, 3 Chapel Street, Chichester, West Sussex, PO19 1BU

Hereinafter "The Emma Red Company" will be referred to as **ERC**.

Introduction

On the 25th May 2018 the General Data Protection Regulation (GDPR) will be applicable and the current Data Protection Act (DPA) will be updated by a new Act giving effect to its provisions. Before that time the provisions of the DPA 1998 will continue to apply.

This Policy sets out the manner in which personal data of Staff, Customers, Suppliers and other individuals will be processed fairly and lawfully.

ERC collects and uses personal information about Staff, Customers, Contractors, Organisations and Suppliers and other individuals who come into contact with the business. This information is gathered in order to enable ERC to provide employment, services related to the business and business to business functions. In addition, there may be a legal requirement to collect and when required supply some information to 3rd Parties.

ERC is both a Data Controller (DC) and a Data Processor (DP) and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, protected, disclosed and destroyed. ERC must be able to demonstrate compliance. Failure to comply with the Principles exposes the Business and Staff to civil and criminal claims and possible financial penalties.

Details of ERC's purpose for holding and processing data can be viewed on the data protection register: <https://ico.org.uk/esdwebpages/search> by entering the business address, name or postcode.

Registration is renewed annually and updated as and when necessary.

Aim

This Policy will ensure that:

ERC processes personal data fairly, lawfully and transparently in compliance with the Data Protection Principles.

All Staff involved with the collection, handling, processing and disclosure of personal data will be aware of their duties and responsibilities.

The data protection rights of those involved with ERC are safeguarded.

Everyone can have confidence in ERC's ability to process data fairly and securely.

Scope

This Policy applies to:

Personal data of all Staff, Clients, Customers, Contractors, Suppliers and any other person carrying out activities on behalf of ERC.

The processing of all personal data whether in manual or electronic form.

The Data Protection Principles

ERC will ensure that personal data will be:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

ERC will be able to demonstrate compliance with these principles.

ERC will have in place a process for dealing with the exercise of the following rights by Staff, Clients, Customers, Contractors and Suppliers in respect of their personal data by providing on lawful request:

- Details of what personal data is held, why it is being processed and who it is shared with.
- Access to their data.
- Correction of inaccuracies.
- Erasure, where the holding of that data is not a statutory or legal requirement
- To restrict processing, where the holding of that data is not a statutory or legal requirement.

There exist further rights to the following:

- Data portability
- Objection to processing
- Not to be subject to automated decision-making technologies including profiling, where the processing of that data is not subject to a statutory or legal requirement

Roles and Responsibilities

The Management & Data Controller (DC) of ERC are responsible for implementing good data protection practices and procedures within the Business and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy.

ERC employs an external ICT Contractor to advise on certain aspects of Data Protection and Security.

Data Security and Data Security Breach Management

All staff are responsible for ensuring that the personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

All staff will comply with the ERC IT use Policy.

Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the Acceptable IT use Policy.

Data will be destroyed securely when no longer required.

New methods of processing personal data including recording technologies which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented by ERC until a Privacy Impact Risk Assessment has been carried out.

ERC will have in place a data breach security management process and serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office (ICO) in compliance with the GDPR.

All staff will be aware of and follow the data breach security management process.

Subject Access Requests

Requests for access to personal data, sometimes referred to as "Subject Access Requests" (SARs) will be processed by the Data Controller. Those making a Subject Access Request will be charged a fee in accordance with current regulations. After 24th May 2018 SARs will be free of charge except where they are "*manifestly unfounded or excessive*" or considered "*repeated*" in which case a charge will be made, this will be advised in advance. A register of all SAR requests will be maintained by the Data Controller.

ERC will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time limit of 40 days continues until 25th May 2018 when under the GDPR the statutory time period reduces to one calendar month on receipt of the request.

Subject Access Requests should be made in writing to the Data Controller.

By email: emma@emmared.co.uk

or in writing to:

Data Controller, The Emma Red Company, 3 Chapel Street, Chichester, West Sussex, PO19 1BU

Sharing Data with 3rd Parties and Data Processing undertaken on behalf of the ERC

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the ERC e.g. by providing cloud based systems or shredding services, the ERC will ensure that there is a written agreement between the Data Controller and Data Processor (3rd Party) requiring the data to be processed in accordance with the Data Protection Principles and in accordance with the DPA.

Ensuring Compliance

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be given to all Staff and a training and documentation matrix will be maintained by the DC.

All staff will read and sign the Acceptable IT use Policy.

ERC advises Clients, Organisations & Customers whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on request and on the website: <https://www.emmared.co.uk>

ERC will ensure that any Privacy Notice(s) contain the following information:

- Contact information for the Data Controller.
- Purpose of processing and legal basis.
- Broad Principles of who we may share data with and why.
- Outline of how long data is retained where appropriate.
- Right to request rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable.